Cyber Security Awareness Training

Why Are You Required to Have Cyber Security Training?

Texas H.B. 3834
Government Code
Section 2054.519 B

- *Full Name (if not common)*
- *Social Security Number*
- *IP Address*
- *Vehicle Plate Number*
- *Drivers License Number*

PII

Personally Identifiable Information

- *Credit Card Number*
- *Date of Birth*
- *Birthplace*
- *Generic Information*
- *Fingerprints, Handwriting, Face*

Cyber Landscape

[Public Sector: 13%]

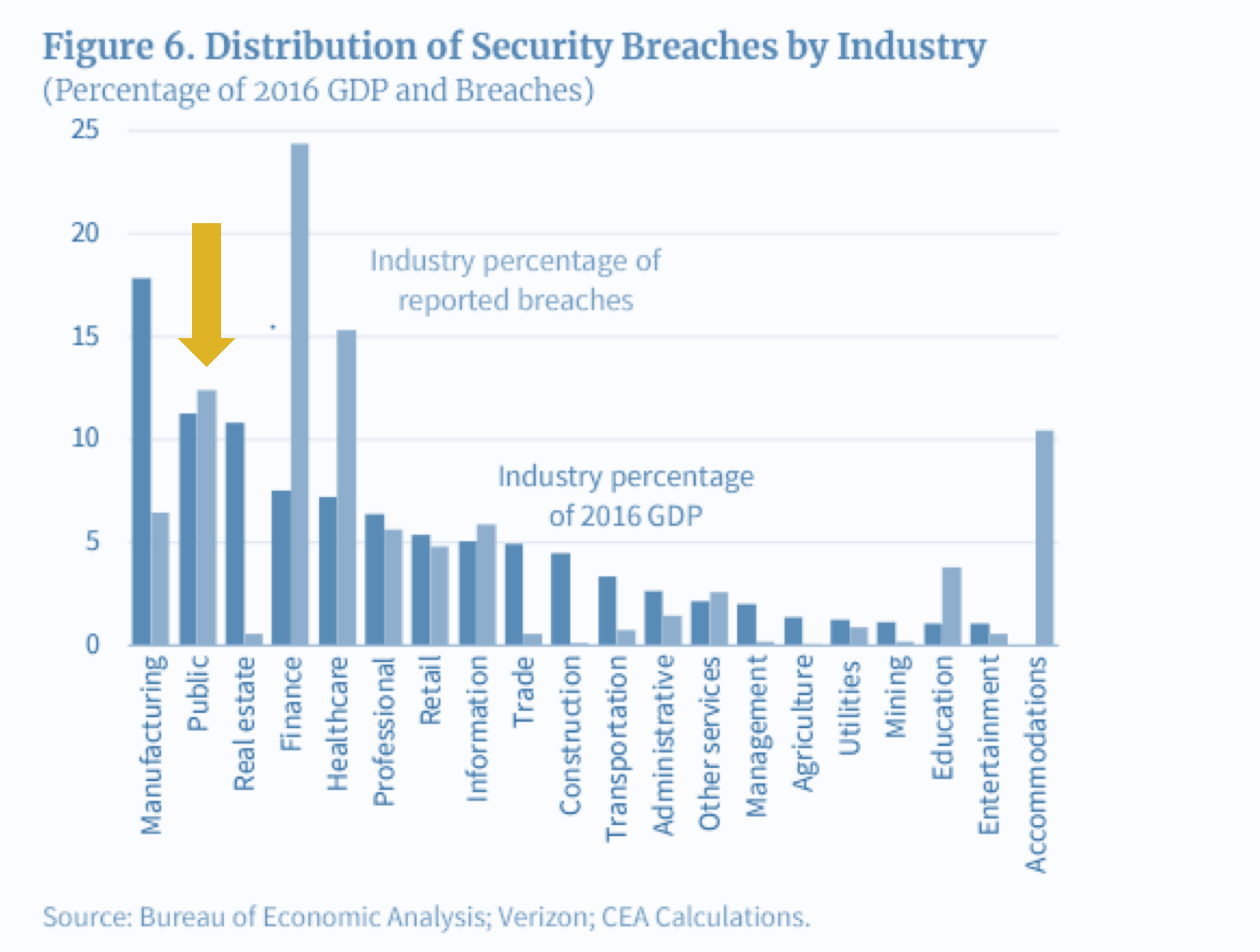


Figure 6. Distribution of Security Breaches by Industry
(Percentage of 2016 GDP and Breaches)

Source: Bureau of Economic Analysis; Verizon; CEA Calculations.

Cyber Landscape

[Top 10 States by Number of Victims & Losses]

#2

Texas

Victims: 21,852

Victims Losses: $115.7M

Cyber Landscape

[Top 10 States Breakdown]

Victims	Losses
CA: 41,974	CA: $214.2M
TX: 21,852	**TX: $115.7M**
FL: 21,837	FL: $110.6M
NY: 17,622	NY: $88.6M
PA: 11,348	MA: $39M
VA: 9,436	WA: $43M
IL: 9,381	IL: $42.9M
OH: 8,157	AZ: $59.4M
CO: 7,909	CO: $39.9M
NJ: 7,657	NJ: $40.4M

**According to FBI ICR*

Principles of Information Security

- Information Security
- Define the different types of information
- What information am I responsible for safeguarding

Data Classification

Sensitive

Data with the most limited access and requires a high degree of integrity. This is typically data that will do the most damage to the organization should it be disclosed

Confidential

Data that might be less restrictive within the organization but might cause damage if disclosed

Private

Usually compartmental data that might not cause damage but must be kept private for other reasons. Ex: Human Resources data

Proprietary

Data disclosed outside the organization on a limited basis or contains information that could impact an organization's competitive advantage, such as the technical specs of a new product

Public

Least sensitive data used by the organization and would cause the least harm if disclosed. Ex: data used for marketing or number of employees

4 Main
Pillars of Cyber Security

Machine Level	Data Level	Network Level	Internet Level

4 Main Pillars of Cyber Security

[Machine Level Pillar]

The Machine Level includes work computers and devices, such as **phones** and **tablets**, or **home computers** that must be **treated with as much care as the data they contain**. The explosion in the use of personal computers and other personal electronic devices has led to innovation and production increases, but this ever-expanding use also creates potential risks.

TML INTERGOVERNMENTAL RISK POOL

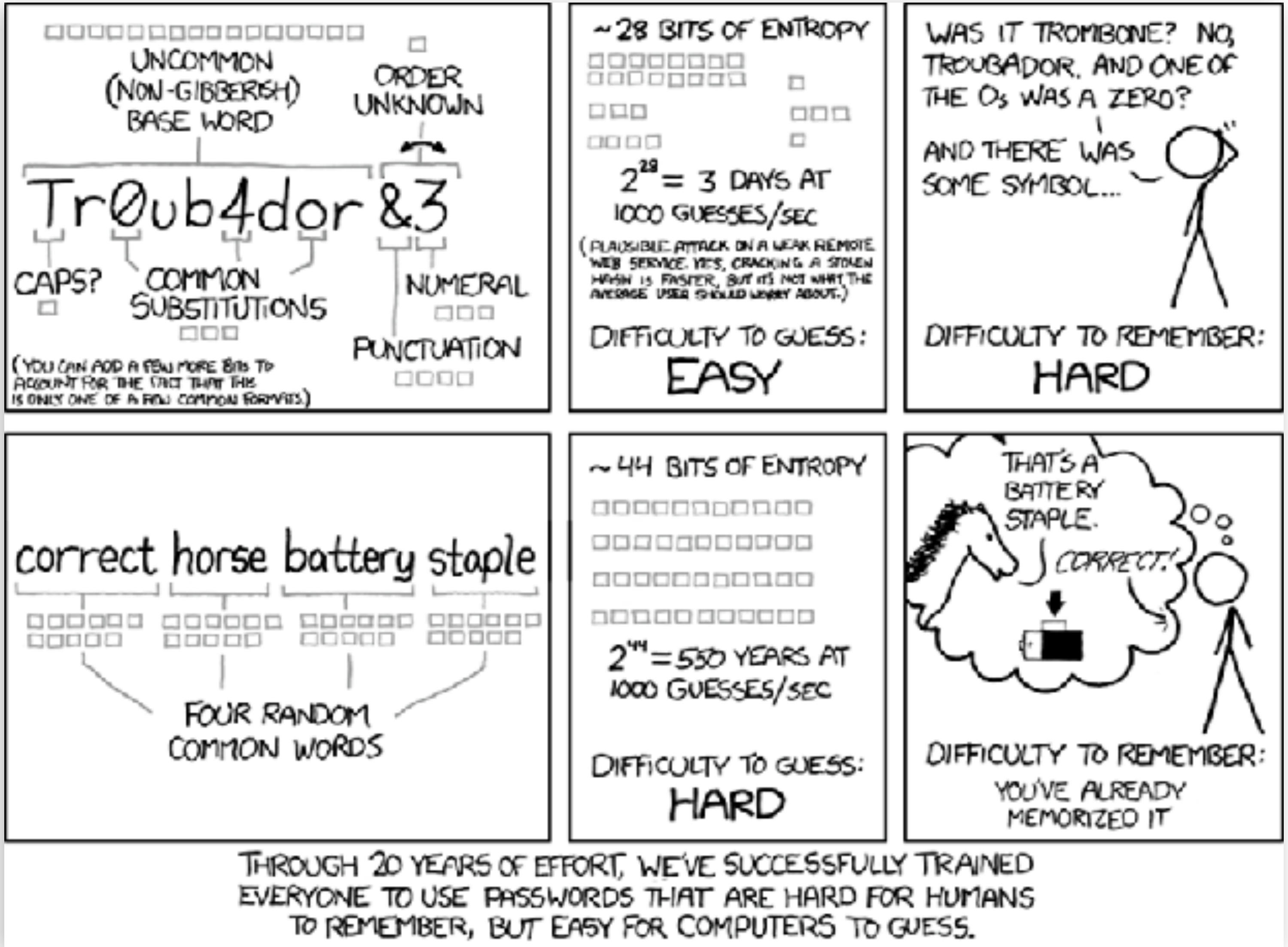
INTEGRITY • PUBLIC SERVICE • FISCAL RESPONSIBILITY • OPERATIONAL EXCELLENCE • PARTNERSHIP TML RISK POOL

4 Main Pillars of Cyber Security

[Machine Level Pillar]

Potential exposures to your organization:

- Weak passwords that are never changed allow hackers access to machines (single word passwords unacceptable)
- Anti-virus software is not installed or not updated
- Employees are not aware of dangers lurking related to cyber security
- Email rules and training are lacking or non-existent (clicking on links or attachments)
- Lack of control of flash drives and other portable connections
- No controls for accessing public Wi-Fi connections
- Lack of administrator controls to prevent downloading of apps or programs onto machines
- Lack of cyber security training


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

4 Main Pillars of Cyber Security

[Data Level Pillar]

The Data Level applies to the quantities, characters or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic, optical or mechanical recording media. The **organization's data must be treated as it is "bundles of cash"** due to the efforts necessary to recreate, if even possible. In simpler terms, "once it's gone it's gone".

4 Main Pillars of Cyber Security

[Data Level Pillar]

Potential exposures to your organization:

- Employees are not aware of the data created by all organizations and the importance of that data or the cost and effort necessary to restore damaged or lost data (if possible, to be restored)
- "Off-site" data backup is not provided, or backups are not performed regularly
- Employees do not believe their organization's data is relevant or "important enough" for a cyber attack
- Organization's data is not encrypted to protect from hackers

4 Main Pillars of Cyber Security

[Network Level Pillar]

The Network Level is becoming all-encompassing as **computers no longer operate on an "island"**, and computers are becoming connected in ways most users do not expect.

Potential exposures to your organization:

- Anti-virus, anti-spyware or anti-malware software or firewalls are not effective
- Daily full system scans are not performed to find, quarantine and remove malicious agents from your network before damage is done
- Off-site backups are not maintained
- Lack of administrator controls of networks

TML INTERGOVERNMENTAL RISK POOL

PARTNERSHIP TML RISK POOL INTEGRITY • PUBLIC SERVICE • FISCAL RESPONSIBILITY • OPERATIONAL EXCELLENCE

4 Main Pillars of Cyber Security

[Internet Level Pillar]

The Internet Level. The “internet of everything” brings people, processes and data to together in a way that was not even imaginable a few years ago. Along with all the positives associated with this new experience, are the exposures and risks created for you and your employer.

4 Main Pillars of Cyber Security

[Internet Level Pillar]

Potential exposures to your organization:

- Almost all devices are now capable of connecting to the internet but there are few controls in some organizations to control how they are connected
- Public wi-fi is used continuously without any concern for potential issues
- Administrators do not control or limit access to the internet
- Work provided devices are used away from work extensively
- Employees are not aware of potential issues and training is not provided

TML INTERGOVERNMENTAL RISK POOL

PARTNERSHIP TML RISK POOL INTEGRITY • PUBLIC SERVICE • FISCAL RESPONSIBILITY • OPERATIONAL EXCELLENCE

Best Practices for Detecting, Assessing, Reporting, & Addressing Threats

Meaning Of Threat

Threat is the potential targeting of a network or system in an attempt to damage, harm or disrupt its capability to operate. This targeting can potentially impact the confidentiality, integrity and availability of the organization’s data.

[*Meaning Of Threat*]

Common types of threats include:

- Theft of confidential, proprietary, or sensitive information
- Modification of existing data, and the compromise of how that data is collected, processed, and stored
- Unauthorized access allowing an external user to gain control of a system to block access to data

What is a “Threat Actor” and What Are Their Goals?

A threat actor is anyone who tries to exploit vulnerabilities in an organization’s systems or users.

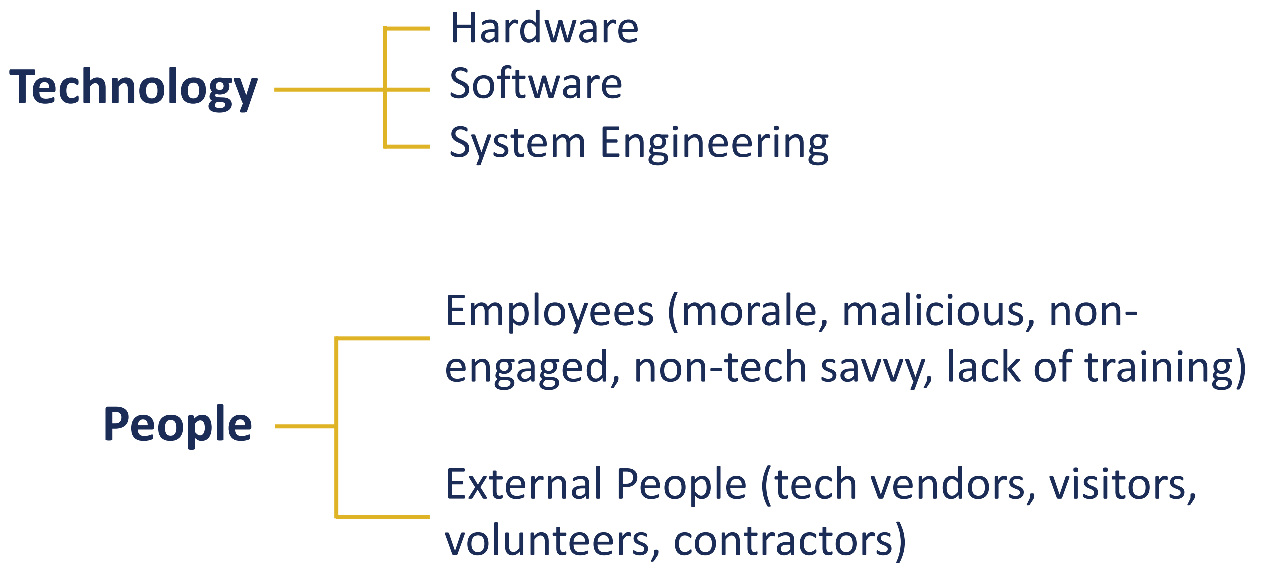
- Profit, financial or otherwise
- Damaging the victim, financially or otherwise
- Damaging the reputation of the victim gathering data that might be used in future attacks
- Gathering data that might be traded or sold to other actors
- Curiosity or malice

Consider This

The idea of a hacker sitting in a dark room deftly finding cracks in firewalls and guessing passwords is still valid, but just as often these days the door is opened for them by unsuspecting users. **Malware sent in infected email attachments still work**, despite the best efforts of anti-virus software companies to stamp it out. Often that is not needed, however. An email containing a link to a website inviting the user to log in to receive an invoice or other enticement is just as likely to succeed by harvesting that user's username and password as someone with advanced technical skill sneaking in through an arcane software vulnerability.

What is meant by "Risk"

Information security risks are choices made by an organization in its technology and people (internal & external)



Technology

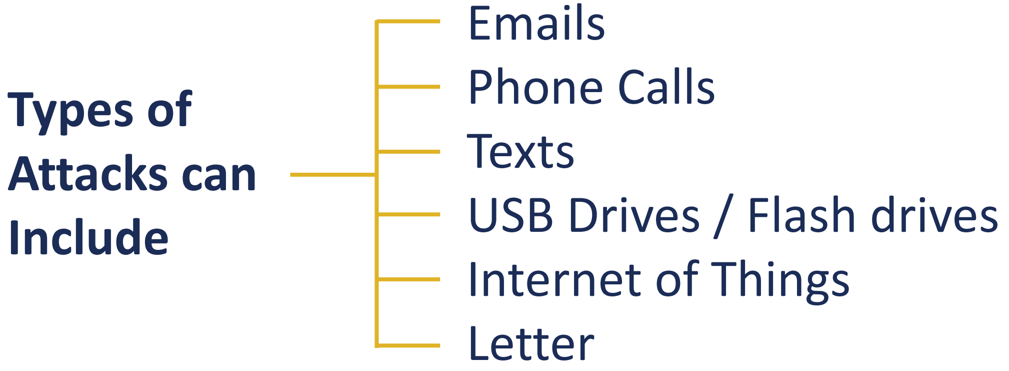
- Hardware
- Software
- System Engineering

People

- Employees (morale, malicious, non-engaged, non-tech savvy, lack of training)
- External People (tech vendors, visitors, volunteers, contractors)

What is meant by “Attack”

Attacks on information security can be defined as any **attempt to gain access or control of** an organization's **data or information systems**, no matter what the level of sophistication


Types of Attacks can Include

- Emails
- Phone Calls
- Texts
- USB Drives / Flash drives
- Internet of Things
- Letter

Types of Tactics Used in an Attack

- Phishing
- Spear Phishing
- Social Engineering
- Whaling
- Malware
- Ransomware
- Vishing (voice phishing)

Recognizing Common Attacks

Malware, covering software with many names like viruses, trojans, worms, backdoors, spyware, and so on, is very common and pernicious. While there are many reputable companies doing excellent work to combat it, it is always true that some get through, especially new formulations that have not yet been recognized. **The risk of user aptitude in how to handle attachments comes into play.** No attachment should be delivered to an inbox without scanning, and a user should not open a document without scanning it again.

Top 10 Tips for Identifying a Phishing Email

1. The message contains a mismatched URL (Uniform Resource Locator)
2. The URL contains a misleading domain name (website name)
3. The message contains poor spelling and/or grammar
4. The message asks for personal information
5. The offer seems too good to be true
6. You didn't initiate the action
7. You're asked to send or provide money or payment
8. The message includes unrealistic threats
9. Something just doesn't look right
10. The email includes an embedded link or attachment that you are asked/tempted to open

TML INTERGOVERNMENTAL RISK POOL

Responding To and Reporting Common Attacks

Responding to an Attack

The common thread to all the attacks outlined previously is the reliance on the user not to question or verify the actions requested. The internet was built on trust, with all the threats present today not even imagined when much of the technology at its core was created. Thus, **responsibility falls on the users and organization** to employ a sustained, suspicious vigilance in any contact.

The most powerful key in any security system is the “delete” key. When a user receives **an email that is even a little suspicious, deleting it is usually the best course of action**. Where possible, verification by calling a known phone number is best. The email might contain a phone number to call in case of questions, but better for the user to find a number independently if not already known.

Responding to an Attack

Many organizations have an IT department, whether a dedicated, in-house team or an outside contractor, and they should be utilized as a resource for validation of suspicion. Any IT professional will say that it’s better to be asked a thousand questions about benign material than to have to eradicate one rampant virus.

Management should be sensitive to user questions and doubts. Without a full-time staff, management should **develop methods for reporting and tracking threat detection**. Without that, an organization might be under continued siege without anyone recognizing it, making improvements to defense impossible.

Responding to an Attack

Attackers might send out a million phishing messages a day with virtually no cost. **Failure to recognize** even one of these **attacks can yield thousands of dollars** to the attackers **and a blow to the reputation** of the organization, not to mention the employee.

Reporting

Users should be aware of how to identify, respond to, and report on threats to information security and suspicious activity

- **Internal Reporting**
  All suspicious activity should be reported according to your internal policy
- **External Reporting**
  Contact all involved parties (contractors, vendors)
- **Cyber crime must be reported to law enforcement**

Training And Policies

Provide external and internal stakeholders with tools needed to ensure **reliability, usability, and security**

- Policies that ensure information security
- Vetting of internal and external stakeholders
- Employee Training Programs
  - ✓ Meets H.B. 3834 Requirements
  - ✓ Awareness Based Training
  - ✓ Internal Policy Training
  - ✓ Ongoing Training (new exposures as identified)

TML INTERGOVERNMENTAL RISK POOL

Conclusion

- Testing/Assessment of Knowledge (Corrected to 100%)
- Sign In Log
- Certificate of Completion (Personnel File)

Free Resources for Public Entities

- TMLIRP members (must login): eriskhub at www.tmlirp.org

- All governmental entities have free access to: https://www.cisecurity.org/ms-isac/